HULFT Square セキュリティホワイトペーパー / HULFT Square Security White Paper

※本セキュリティホワイトペーパーは、他の言語に翻訳され、日本語による本セキュリティホワイトペーパーとその他の言語による翻訳版の間に相違がある場合には、日本語による記述があらゆる点について優先します。
*If this Security White Paper is translated into other languages, and there is any discrepancy between the Japanese version of the Security White Paper and any translated version in any other language, the Japanese version shall prevail in all respects.

改訂履歴 / Revision History

版数 / Revision	発行日 / Date of Issue	変更内容 / Changes
初版 / Rev. 1.0	June 8th, 2022	
2版 / Rev. 2.0	August 17th, 2022	①誤りの訂正(EC2→EKS Fargate) ②用語の統一(解約日→契約終了日) ①EC2 → EKS Fargate ②Termination Date → Contract End Date
3版 / Rev. 3.0	February 8th, 2023	①バージョンアップに伴う実施内容の変更の反映 ②文章表現の変更 ①Changes in implementation details for version upgrades ②Changes in text wording

この HULFT Squareセキュリティホワイトペーパー（以下「本書」といいます。）は、 株式会社セゾンテクノロジー（以下「当社」といいます。）が提供するiPaaS型クラウドサービス「HULFT Square」のインフラストラクチャー及びアプリケーションにどのようなセキュリティ対策を施しているかを紹介するドキュメントです。

1. 当社の取組み

⑴ 情報セキュリティ方針

当社は、情報セキュリティ基本方針を定めております。詳細は下記URLをご確認ください。

https://www.saison-technology.com/security

また、当社は情報セキュリティマネジメントシステム（ISMS）の国際規格ISO/IEC27001:2013認証を取得しています。

⑵ 情報セキュリティインシデント対応体制

情報セキュリティインシデント発生時、連絡窓口、社内の責任体制と対応手順を定めています。

2. HULFT Squareに関するセキュリティ対応

⑴ クラウドコンピューティング 環境

HULFT Square はクラウドコンピューティング環境として Amazon Web Services （「AWS」）の Amazon Elastic Compute Cloud（Amazon EKS Fargate）を採用しています。

クラ ウドコンピューティング環境のセキュリティ対策については、下記URLをご確認ください。

AWS Security Center

https://aws.amazon.com/security/?nc1=h_ls

⑵ 機密性

HULFT Squareは通信の機密性を確保するために、HULFT Squareとクライアント間の通信はSHA256 アルゴリズム対応の SSL 証明書による通信データの暗号化を常時適用します。また、登録済みアカウントや接続情報の不正利用を防ぐ目的で、HULFT Squareはアカウントパスワードや接続パスワードをハッシュ化して保持します。サービスに格納されるデータは電子政府推奨暗号リストに含まれる「AES-256」のアルゴリズムにて暗号化されます。

⑶ 可用性

HULFT Squareでは、同一リージョン内でマルチAZの構成をとる等の可用性を確保しています。

⑷ 開発工程におけるセキュリティ対策

HULFT Squareの開発は当社が指定したセキュリティの担保された環境下で行っています。

ソースコードの脆弱性を早期に発見するために、開発工程において 静的ソース解析ツール及び疑似攻撃型脆弱性診断ツールによる検証を実施しています。 開発環境、ステージング環境、プロダクション環境（お客様がご利用になる環境） をそれぞれ用意し、未検証のアプリケーションをプロダクション環境にデプロイしない仕組みを導入しています。また、定期的な脆弱性検査および対応の実施を開発プロセスに取り入れています。

3. オペレーション対応

⑴ ペネトレーションテスト

HULFT Squareでは、外部機関によるペネトレーションテスト実施しています。実施インターバルは年に一度を計画しています。

⑵ モニタリング

当社は、HULFT Squareに対する外部からの不正侵入対策および、全体に関わる共通システムの監視(死活監視、CPU/メモリ監視)を行います。
自動モニタリングシステムを活用して、異常検知時または警戒閾値を越えた場合、当社の運用担当者及び開発者に情報の通知を行い、内容に応じ当社よりお客様にご連絡します。
お客様にて作成頂くHULFT IntegrateやHULFT Transferサービス(インスタンス)の監視はお客様にて行って頂くようお願いします。

⑶ インシデント管理

HULFT Squareにおいて重大障害等インシデントが発生した場合、通常の問い合わせ・運用対応時のものとは別にインシデント管理手順により対応します。お客様には、HULFT Squareステイタスサイト等で情報を発信します。

⑷ アクセスコントロール

① お客様情報の保管
お客様の情報はHULFT Square内に暗号化され保管されています。外部からアクセス可能なゾーンへの配置はありません。

② サイバー攻撃対策
HULFT Square は当社内外問わず悪意のあるユーザーからのサイバー攻撃（DDoS攻撃等）を防ぐために、その脅威検知と防御を行っています。

③ 不正アクセス対策
事前に許可されたユーザーだけが HULFT Squareにアクセスできる仕組みとなり、パスワード認証の他、スマートフォンを利用した多要素認証を導入しています。また、管理サーバへのアクセスを当社内からの通信に限定することで、 故意・過失による不正アクセスの可能性を抑制しています。

④ 当社従業員の管理
当社全ての従業員（協力会社社員含めて）に対して入社時（受入れ時）のセキュリティ教育および定期的なセキュリティ教育を行っています。事務所への入退出管理など物理的なセキュリティ対策を実施し、情報処理装置を保護しています。

4. データの取扱い

⑴ バックアップ

システムのバックアップを1回/日の頻度で実施しています。

⑵ ロギング

お客様の操作ログは１ヶ月間の保管をいたします。

⑶ 解約後の取扱い

お客様が契約解除をされた場合、契約終了日以降は本サービスにアクセスできなくなります。契約終了時点で本サービス内に残ったデータは契約終了日以降に削除されます。再度、契約され利用を再開された場合も元に戻すことはできません。

5. リスクマネジメントと保険

当社は、IT業務賠償責任保険を付保しています。

6. 通知

本書は、本書の発行日時点での情報を記述しており、これらは事前通知なく変更される場合があります。最新の情報については、下記URLをご確認ください。

HULFT Squareサービス仕様書 別添３「セキュリティホワイトペーパー」
https://www.hulft.com/download_file/17363

お客様は、本書の情報およびHULFT Squareの使用について独自に評価する責任を負うものとします。これらの情報は明示または黙示を問わずいかなる保証も伴うことなく「現状のまま」提供されるものです。

以上

This HULFT Square Security White Paper ("this document") is a document that introduces the security measures implemented in the cloud service "HULFT Square" infrastructure and applications provided by Saison Technology Co., Ltd. ("the Company")

1. The Company's Initiatives

1.1 Information Security Policies

The company has established a basic policy for information security. Please refer to the following URL for details.
https://www.saison-technology.com/security
In addition, the Company has obtained "ISO/IEC27001:2013" certification, the international standard for ISMS (Information Security Management System) accreditation.

1.2 Information Security Incident Handling

In the event of an information security incident, a contact point, internal responsibility structure, and response procedures are established.

2. Security measures for HULFT Square

2.1 Cloud Computing Environment

HULFT Square uses Amazon Web Services ("AWS") and Amazon Elastic Compute Cloud ("Amazon EKS Fargate") as its cloud computing environment.
Please refer to the following URL for security measures of the cloud computing environment.
AWS Security Center
http://aws.amazon.com/security/

2.2 Confidentiality

To ensure the confidentiality of communications, HULFT Square always encrypts communication data between HULFT Square and the client using SSL certificates supporting the SHA256 algorithm. In addition, to prevent unauthorized use of the registered account and connection information, HULFT Square maintains a hashed version of account and connection passwords. Data stored in the service will be encrypted with the "AES-256" algorithm, included in the e-government recommended cipher list.

2.3 Availability

HULFT Square has a multi-AZ configuration within the same region to ensure availability.

2.4 Security Measures in The Development Process

HULFT Square is developed in a secure environment specified by the Company.
To detect vulnerabilities in source code at an early stage, we conduct verification using static source analysis tools and pseudo-attack type vulnerability diagnostic tools during the development process. HULFT Square provides a development environment, a staging environment, and a production environment (customer's environment); a mechanism is introduced to prevent deploying untested applications to the production environment. We also incorporate regular vulnerability inspections and handling into our development process.

3. Operation

3.1 Penetration Test

HULFT Square conducts penetration testing by an external institution. The implementation interval is planned to be once a year.

3.2 Monitoring

The Company will provide countermeasures against unauthorized access to HULFT Square from outside

and monitor the entire common system (dead/alive monitoring, CPU/memory monitoring).
If any anomalies are detected or alarm thresholds are exceeded, the Company will notify our operations staff and developers, who will, in turn, contact customers.
Monitoring HULFT Integrate and HULFT Transfer services (instances) created by a customer is the customer's responsibility.

3.3 Incident Management

In the event of a significant failure or other incident at HULFT Square, the incident will be handled in accordance with incident management procedures separate from those used for normal inquiries and operational support. Information will be sent to customers via the HULFT Square status site.

3.4 Access Control

3.4.1 Storage of Customer Information

Customer information is encrypted and stored within HULFT Square.
It is not placed in an externally accessible zone.

3.4.2 Cyber Attack Prevention

HULFT Square provides threat detection and protection against cyber-attacks (e.g., DDoS attacks) from malicious users, both internal and external to the Company.

3.4.3 Measures against Unauthorized Access

Only pre-approved users can access HULFT Square. Password authentication, as well as multi-factor authentication using smartphones, are introduced. In addition, limiting access to the management server to communications from internal sites reduces the possibility of unauthorized access due to intentional or negligent acts.

3.4.4 Management of Employees

The Company provides security education to all the employees (including employees of subcontractors) when they join the company (upon receiving their employment) and regularly. We implement physical security measures such as access control to the office to protect information processing equipment.

4. Data

4.1 Backup

System backups are performed once a day.

4.2 Logging

Customer operation logs will be kept for one month.

4.3 After Termination

If a customer cancels the contract, the customer will not be able to access the service after the contract termination date. Any data remaining in the service at the time of contract termination will be deleted after the contract termination date. The data cannot be restored even if the customer resumes the contract and resumes the use of the service.

5. Risk Management and Insurance

The Company carries IT business liability insurance.

6. Notification

This document describes information as of publication date, which is subject to change without prior notice. Please refer to the following URL for the latest information.
HULFT Square Service Specification Attachment 3

"HULFT Square Security White Paper"
https://www.hulft.com/download_file/17363
Customers are solely responsible for their independent evaluation of the information in this document and their use of HULFT Square. The information is provided "as is" without warranty, either express or implied.